



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/566,206	06/05/2006	Kezhi Qiao	00698000001	5525
22907 7590 05/23/2007 BANNER & WITCOFF, LTD. 1100 13th STREET, N.W. SUITE 1200 WASHINGTON, DC 20005-4051			EXAMINER LAFORGIA, CHRISTIAN A	
			ART UNIT 2131	PAPER NUMBER
			MAIL DATE 05/23/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/566,206	QIAO ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Christian La Forgia	2131	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 27 January 2006.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-7 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-7 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 27 January 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)            | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. _____                                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>1/27/06</u> .   | 6) <input type="checkbox"/> Other: _____                          |

### **DETAILED ACTION**

1. Claims 1-7 have been presented for examination.

#### ***Priority***

2. Acknowledgment is made of applicant's claim for foreign priority. A certified translation is required by the Examiner to eliminate the potential use of intervening reference U.S. 2006/0274899 to Zhu et al.

#### ***Information Disclosure Statement***

3. The information disclosure statement filed 27 January 2006 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document, in this case WO 02054201; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.
4. The information disclosure statement (IDS) submitted on 27 January 2006 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner has considered the information disclosure statement.

#### ***Specification***

5. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.
6. The following title is suggested: Authentication Method for Media Gateway.

#### ***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2131

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 1, 3, and 5-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S.

Patent Application Publication No. 2005/0220078 to Luken, hereinafter Luken, in view of U.S.

Patent Application Publication No. 2002/0016913 to Wheeler et al., hereinafter Wheeler.

9. As per claim 1, Luken teaches a system comprising a media gateway (Figure 1 [blocks 26 and 40]) and a Media Gateway Controller (Figure 1 [blocks 36, 44]). Luken also discloses that the Media Gateway Controller can be used to verify digital signatures (paragraph 0064), which are based on keys.

10. Luken does not teach generating a session key based on the digital signature to be used to communicate between the two devices and renewing a session key when the previous session key has expired.

11. Wheeler discloses generating a session key from a digital signature and using it to communicate (claim 14). Updating or renewing the key upon its expiration would have required only routine skill in the art and official notice is taken of such.

12. It would have been obvious to one of ordinary skill in the art at the time the invention was made to create a session key from a digital signature and use it for secure communication, since Wheeler states at paragraphs 0380-0387 that the use of a session key based on the digital signature will protect against fraudulent displays, protect account information and protect against replay attacks.

Art Unit: 2131

13. Regarding claim 3, Luken teaches for each call, attaching a digital signature to each call message from said Media Gateway Controller to said Media Gateway by using said shared key (paragraph 0064);

validating said digital signature in said call message in said Media Gateway by using said shared key, and if it is valid, returning a response message attached with a digital signature using said shared key to said Media Gateway Controller (paragraph 0064); and

validating said digital signature in said response message in said Media Gateway Controller by using said shared key, if it is valid, setting up a call service (paragraph 0020, i.e. establishing a connection), otherwise denying the call (paragraph 0022, i.e. rejection message).

14. With regards to claim 5, Luken teaches that the algorithm used to generate a shared key by said Media Gateway Controller and said Media Gateway is different from the algorithm used to generate a digital signature by said Media Gateway Controller and said Media Gateway (paragraph 0064, i.e. Algorithm field).

15. With regards to claim 6, Luken teaches that a field/packet of an expanded protocol is used to transmit said parameter for generating a shared key and said digital signature (paragraph 0064, i.e. key and digital signature).

16. Regarding claim 7, Wheeler teaches the use of a session key which includes a lifetime the key that is either time or the number of times said shared key can be used for authentication and Official Notice is taken of such.

17. Claims 2 and 4 rejected under 35 U.S.C. 103(a) as being unpatentable over Luken in view of Wheeler as applied to claim 1 above, and further in view of **Cryptography and Network Security**, by William Stallings, hereinafter Stallings.

18. Regarding claims 2 and 4, Luken teaches generating a new shared key further comprises: initiating a register signaling from said Media Gateway to said Media Gateway Controller to register, wherein said register signaling has a parameter for generating a shared key and a digital signature generated by said initial key (paragraph 0064).

19. Wheeler teaches generating a shared key and setting up a lifetime of said shared key after said Media Gateway Controller has validated said Media Gateway with said initial key (claim 14). Wheeler teaches the use of a session key which has a lifetime and Official Notice is taken of such.

20. Neither Wheeler and Luken teach initiating a modification command from said Media Gateway Controller to said Media Gateway, wherein said modification command has a parameter for generating the shared key, a digital signature generated by said initial key and a lifetime of a shared key; and generating the shared key and setting up the lifetime of said shared key after said Media Gateway has validated said Media Gateway Controller with said initial key.

21. It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate a new shared key, since Stallings states at page 216 that the more frequently the session key are exchanged, the more secure they are, because the opponent has less ciphertext to work with for any given session key.

*Conclusion*

22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

23. The following patents are cited to further show the state of the art with respect to media gateway control protocol, such as:

United States Patent Application Publication No. 2004/0255158 to Lin et al., which is cited to show client security authentication with media gateway controllers.

United States Patent Application Publication No. 2002/0087858 to Oliver et al., which is cited to show authentication and verification in media gateways.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

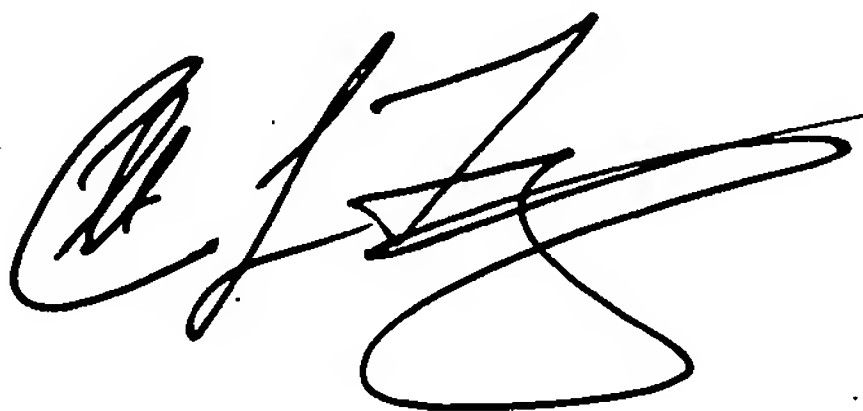
25. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.



Art Unit: 2131

26. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia  
Patent Examiner  
Art Unit 2131

A handwritten signature in black ink, appearing to read 'CLF', with a large, stylized flourish at the end.

clf